National Infrastructure Protection Center
CyberNotes

Issue #2002-18 *September 9, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between August 20 and familiar September 5, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Aestiva[1]	Multiple	HTML/OS 2.4	A Cross-Site Scripting vulnerability exists because metacharacters are not properly sanitized from error message output, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	HTML/OS Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploits have been published.

[1] Bugtraq, September 3, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
AFD[2]	Multiple	AFD 1.2-1.2.14	Several buffer overflow vulnerabilities exist due to insufficient bounds checking of user supplied values for the working directory, which could let a malicious user execute arbitrary code as root.	Upgrade available at: http://www.dwd.de/AFD/download/src-1.2.15.tar.gz Patch available for version 1.2.14 is located at: ftp://ftp.dwd.de/pub/afd/patch-1.2.15.bz2	Multiple AFD Working Directory Buffer Overflows	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Alan Ward[3]	Windows	A-Cart 2.0	A vulnerability exists because the database file is stored in the web directory, which could let a remote malicious user download the database file via a HTTP request.	No workaround or patch available at time of publishing.	A-Cart Web Accessible Database File	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Belkin[4]	Multiple	F5D6130	A remote Denial of Service vulnerability exists when a malicious user issues a small number of SNMP 'GetNextRequest' requests.	No workaround or patch available at time of publishing.	F5D6130 Wireless Network Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with commonly available tools.
Blue Coat Systems[5]	Multiple	CacheFlow Client Accelerator 4.1.06 & prior, Security Gateway 2.1.02 & prior, Server Accelerator 4.1.06 & prior	A Cross-Site Scripting vulnerability exists because the error pages may allow the display of certain characters used in HTML tags, which could let a malicious user execute arbitrary script code.	Updated custom error pages file and instructions available at: http://download.cacheflow.com/release/CA/3.1.00-docs/v3.1-error-pages.zip and http://download.cacheflow.com/release/CA/4.0.00-docs/CA4-error-pages.zip and http://download.cacheflow.com/release/SA/4.0.00-docs/SA4-error-pages.zip	Blue Coat Systems Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Caldera[6]	Unix	OpenUnix 8.0, UnixWare 7.1.1	Two vulnerabilities exist: a vulnerability exists because privileges are not dropped before the 'xkbcomp' command or other external commands are invoked, which could let a malicious user execute arbitrary commands with elevated privileges; and a buffer overflow vulnerability exists in the 'xkbcomp' code, which could let a malicious user execute arbitrary code.	Update available at: ftp://ftp.sco.com/pub/updates/OpenUNIX/CSSA-2002-SCO.38	Caldera X 'xkbcomp' Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proofs of Concepts exploits have been published.

[2] Netric Security Team Advisory, September 4, 2002.
[3] SecurityFocus, August 30, 2002.
[4] Securiteam, August 27, 2002.
[5] Blue Coat Systems Security Advisory, September 3, 2002.
[6] SCO Security Advisory, CSSA-2002-SCO.38, August 27, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Cerulean Studios[7]	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.73, 0.725, 0.6351	A buffer overflow vulnerability exists in the XML parser when a specially-crafted skin file is created that contains an overly large "colors file" field, which could let al remote malicious user cause a Denial of Service or possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Trillian Skins Colors Buffer Overflow	Low/**High** **(High if arbitrary code is executed)**	Bug discussed in newsgroups and websites.
Check Point Software[8]	Multiple	Firewall-1 4.0, 4.0 SP1-SP8, 4.1, 4.1 SP1-SP5, Firewall-1 (VPN+ DES + STRONG)] 4.1 SP2 Build 41716, 4.1 Build 41439, (VPN + DES) 4.1, Next Generation, Next Generation FP1&FP2	A vulnerability exists because different responses are sent when Phase-1 aggressive mode IKE packets are received that contain valid and invalid usernames, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Check Point Firewall-1 SecuRemote IKE Username Guessing	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Cisco Systems[9]	Windows	VPN Client 2.0, 3.0, 3.1, 3.5.1 for Windows	A vulnerability exists because it is possible to extract the plaintext password value from the authentication property page, which could let a malicious user obtain sensitive information.	The procedure to upgrade on the various platforms to the fixed software version is detailed in the documentation available at: http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/	VPN Client Password Disclosure	Medium	Bug discussed in newsgroups and websites.
Cisco Systems[10]	Windows, Unix, MacOS X 10.1.0 or later	VPN Client 2.0, 3.0, 3.0.5, 3.1, 3.5.1 for Windows, VPN Client 3.5.1 for Solaris, 3.5.1 for Mac OS X, 3.5.1 for Linux	A vulnerability exists because the VPN Client does not have the ability to verify that specific certificate Distinguished Names (DN) fields match in the certificate received from the VPN Concentrator, which could let certificates supplied by a malicious host be trusted.	The procedure to upgrade on the various platforms to the fixed software version is detailed in the documentation available at: http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/	VPN Client Distinguished Name Validation	Medium	Bug discussed in newsgroups and websites.

[7] Bugtraq, August 31, 2002.
[8] Securiteam, September 3, 2002.
[9] Cisco Security Advisory, September 5, 2002.
[10] Cisco Security Advisory, September 5, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Cisco Systems[11]	Windows, Unix, MacOS X 10.1.0 or later	VPN Client 2.0, 3.0, 3.0.5, 3.1, 3.5.1C, 3.5.1 for Windows, VPN Client 3.5.1, 3.5.2 for Solaris, VPN Client 3.5.1, 3.5.1 for Mac OS X, VPN Client 3.5.1, 3.5.2 for Linux	A vulnerability exists due to weak random number generation, which could let a malicious user mount a man-in-the middle attack or possible inject arbitrary packets into a connection.	The procedure to upgrade on the various platforms to the fixed software version is detailed in the documentation available at: http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/	VPN Client Random Number Generation	Medium	Bug discussed in newsgroups and websites.
Cisco Systems[12]	Windows, Unix, MacOS X 10.1.0 or later.	VPN Client 2.0, 3.0, 3.0.5, 3.1, 3.5.1C, 3.5.1,3.5.2, 3.6 (Rel), 3.6 for Windows, VPN Client 3.5.1, 3.5.2, 3.6 for Solaris, 3.5.1, 3.5.2, 3.6 for Mac OS X, VPN Client 3.5.1, 3.5.2, 3.6 for Linux	A vulnerability exists when a system is configured for the all tunnel mode (and the split tunneling mode is disabled) because a TCP packet can be acknowledged via the tunnel-assigned IP, which could let a malicious user obtain sensitive information.	The procedure to upgrade on the various platforms to the fixed software version is detailed in the documentation available at: http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/	VPN Client All Tunnel Mode Information Leakage	Medium	Bug discussed in newsgroups and websites.
Cisco Systems[13]	Windows	VPN Client 2.0, 3.0 for Windows	A remote Denial of Service vulnerability exists when a malicious user sends NETBIOS TCP packets that have their source and destination ports set to 137;	The procedure to upgrade on the various platforms to the fixed software version is detailed in the documentation available at: http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/	Cisco VPN Client NETBIOS TCP Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[11] Cisco Security Advisory, September 5, 2002.
[12] Cisco Security Advisory, September 5, 2002.
[13] Cisco Security Advisory, September 5, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Cisco Systems[14]	Multiple	Cisco VPN 3000 Concen-trator 2.5.2 (A)-(C) & (F), 3.0.3 (A), 3.1.1, 3.5 (Rel), 3.5.3, 3.5.4, 3.6 (Rel), VPN 3002 Hardware Client	Numerous vulnerabilities exist in the VPN 3000 series concentrators and VPN 3002 Hardware Client, which could let a local/remote malicious user obtain unauthorized access to the network, obtain sensitive information or initiate a Denial of Service.	For more information, workarounds and patches, see advisory located at: http://www.cisco.com/warp/public/707/vpn3k-multiple-vuln-pub.shtml.	Multiple Cisco VPN 3000 Vulnerabilities	Low/ Medium (Medium if unauthorized access is obtained or sensitive informa-tion is obtained)	Bug discussed in newsgroups and websites. Some of these vulnerabilities can be exploited via a web browser and no exploit code is required for some. Vulnerability has appeared in the press and other public media.
Compaq Computer Corpora-tion[15]	Unix	Digital Unix 4.0f, Tru64 4.0g PK3 (BL17), 4.0g, 4.0f PK7 (BL18), 4.0f PK6 (BL17), 4.0f, 5.0a PK3 (BL17), 5.0a, 5.0 PK4 (BL17 & 18), 5.1a PK2 (BL2), 5.1a PK1 (BL1), 5.1a, 5.1 PK5 (BL19), 5.1 PK4 (BL18), 5.1 PK3 (BL17), 5.1	Several vulnerabilities exist: a Denial of Service vulnerability exists in /ur/sbin/ping; and several buffer overflow vulnerabilities exist in various binaries, which could let a unauthorized user obtain privileged access, cause a Denial of Service, or execute arbitrary code.	Patches available at: ftp://ftp1.support.compaq.com/public/unix/	Tru64 UNIX Multiple Local and Remote Buffer Overflow	Low/**High** **(High if arbitrary code is executed)**	Bug discussed in newsgroups and websites. Exploit has been published.
Comput-alynx[16]	Windows 95/98/NT 4.0	CMail 2.4, 2.4.7, 2.4.12 AV, 2.4.12	A Denial of Service vulnerability exists because some of types of requests are not handled properly.	No workaround or patch available at time of publishing.	CMail POP3 Denial Of Service	Low	Bug discussed in newsgroups and websites.

[14] Cisco Security Advisory, September 3, 2002.
[15] Compaq Compute Corporation Advisory, SSRT2275/SSRT2229:, August 30, 2002.
[16] Bugtraq, August 30, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Dan Mueth[17, 18, 19]	Unix	Scroll Keeper 0.3, 0.3.1, 0.3.4-0.3.6, 0.3.11	A vulnerability exists because the 'scrollkeeper-get-cl' program creates temporary files in an insecure manner in /tmp, which could let a malicious user create arbitrary files and execute arbitrary commands.	**RedHat:** ftp://updates.redhat.com/ **Debian:** http://security.debian.org/pool/updates/main/s/scrollkeeper/ **Gentoo Linux:** Users who are running app-text/scrollkeeper-0.3.11 and earlier update their systems as follows: emerge rsync emerge scrollkeeper emerge clean	ScrollKeeper Tempfile Symbolic Link CVE Name: CAN-2002-0662	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Desiderata Software[20]	Multiple	Blazix 1.2, 1.2.1	Two vulnerabilities exist: a vulnerability exists because special characters are not properly handled when they are appended to requests, which could let a malicious user obtain sensitive information; and a vulnerability exists when a request is passed to the web server that ends in a certain special character, which could let a malicious user obtain sensitive information.	Patch available at: http://www.blazix.com	Blazix Special Character Handling	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Ekilat LLC[21]	Multiple	php (Reactor) 1.2.7 pl1	A vulnerability exists because HTML is not properly sanitized from various fields, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	PHPReactor HTML Injection	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Ethereal Group[22, 23, 24, 25]	Windows 95/98/ME/ NT/ 4.0/2000, XP, Unix	Ethereal 0.9.0-0.9.5	A buffer overflow vulnerability exists in the ISIS protocol dis-sector, which could let a malicious user execute arbitrary code.	**Ethereal Group:** http://www.ethereal.com/distribution/ethereal-0.9.6.tar.gz **RedHat:** ftp://updates.redhat.com/	Ethereal ISIS Dissector Memory Corruption	**High**	Bug discussed in newsgroups and websites.

[17] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:186-07, August 28, 2002.
[18] Debian Security Advisory, DSA 160-1, September 3, 2002.
[19] Gentoo Linux Security Announcement, September 4, 2002.
[20] PivX Security Advisory, August 24, 2002.
[21] Bugtraq, August 24, 2002.
[22] Ethereal Security Advisory, enpa-sa-00006, August 20, 2002.
[23] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:169-13, August 28, 2002.
[24] FreeBSD Security Notice, FreeBSD-SN-02:05, August 28, 2002.
[25] Gentoo Linux Security Announcement, August 30, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Facto System[26]	Windows	Weblog 0.9b, 1.0 Beta, 1.1 Beta	Multiple SQL injection vulnerabilities exist because the script fails to validate numeric data or fails to properly escape certain control characters in strings, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Weblog Multiple SQL Injection	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Finjan Software[27]	Windows NT 4.0/2000	SurfinGate 6.0, 6.0 1	Two vulnerabilities exist: a vulnerability exists because host and domain names are not resolved by default, which could let a malicious user access a site by entering the IP address; and a vulnerability exists because trailing characters are not handled properly, which could let a malicious user access a site by entering the host and domain name with a trailing character.	The vendor has confirmed the existence of this issue, and stated that the system is not designed to function as a strong blacklist, as documented in the help file. However, the vendor has made it known that this functionality will be added in addition to resolution of this issue in a future release.	SurfinGate URL Filter Bypassing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
FreeBSD [28]	Unix	AIDE Port 0.7_1	A vulnerability exists in the default configuration file in the AIDE port because subdirectories are not adequately checked, which could let a malicious take arbitrary actions against the system without detection	Upgrade available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/All/	FreeBSD AIDE Port Default Configuration File	Medium	Bug discussed in newsgroups and websites.
GDAM[29]	Unix	GDAM 0.933, 0.942	A buffer overflow vulnerability exists in the filename option commandline when handling an overly long filename, which could let a malicious user obtain elevated privileges via the execution of arbitrary code.	No workaround or patch available at time of publishing.	GDAM123 Filename Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Hewlett Packard Systems[30]	Unix	HP-UX 10.20, 11.0, 11.11	Two vulnerabilities exist: a buffer overflow vulnerability exists in the LP subsystem, which could let a malicious user cause a Denial of Service; and a buffer overflow vulnerability exists in the lp spool commands, which could let a malicious user obtain elevated privileges.	Patches available at: http://itrc.hp.com Patch PHCO_27133, Patch PHCO_27132, Patch PHCO_27020	HP-UX LP Subsystem & LP Spool Commands Vulnerabilities	Low	Bug discussed in newsgroups and websites.

[26] Bugtraq, August 31, 2002.
[27] Bugtraq, September 4, 2002.
[28] FreeBSD Security Notice, FreeBSD-SN-02:05, August 28, 2002.
[29] Netric Security Team, August 27, 2002.
[30] Hewlett-Packard Company Security Bulletin, HPSBUX0208-213, August 27, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Hewlett Packard Systems[31]	Unix	HP-UX 11.0	A vulnerability exists in the VJE.VJE-RUN file set used to provide VJE Japanese Input support, which could let a malicious user obtain elevated privileges. This vulnerability exists if VJE.VJE-RUN has ever been installed on the system, even if has been removed.	**Temporary workaround:** http://www-1.ibm.com/services/continuity/recover1.nsf/MSS/MSS-OAR-E01-2002.627.1	HP-UX VJE.VJE-RUN Default Path Modification	Medium	Bug discussed in newsgroups and websites.
Indepen-dent Solution[32]	Multiple	Simple Site Searcher, Super Site Searcher	A vulnerability exists because shell metacharacters are not adequately filtered from query string parameters in a request to the search engine script, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Super Site Searcher Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Jacques Gelinas[33]	Unix	Linuxconf 1.1.6r10, 1.1.7, 1.1.8, 1.1.9r2, 1.1.9r1, 1.2r2, 1.2r1, 1.2, 1.2.1r1-r8, 1.2.1, 1.2.2, 1.2.3r1&2, 1.2.3, 1.2.4r2, 1.2.4r4, 1.2.4r5, 1.2.4, 1.27r5, 1.27r4, 1.27r3, 1.27, 1.28r1-r3, 1.28	A buffer overflow vulnerability exists in the LINUXCONF_LANG environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code with root permissions	Upgrade available at: http://www.solucorp.qc.ca/linuxconf/	Linuxconf Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Kerio[34]	Windows NT 4.0/2000	Personal Firewall 2 2.1-2.1.4	A Denial of Service vulnerability exists when a malicious user sends a large number of SYN packets to the host.	No workaround or patch available at time of publishing.	Personal Firewall Denial of Service	Low/**High** **(High if DoS best practices not in place)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[31] Hewlett-Packard Company Security Bulletin, HPSBUX0208-214, August 28, 2002.
[32] SecurityFocus, September 3, 2002.
[33] iDEFENSE Security Advisory:, August 28, 2002.
[34] NSSI-Research Labs Security Advisory, NSSI-2002-keriopfw, August 28, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Khaled Mardam-Bey[35]	Windows 95/98/ME/ NT 4.0/2000, XP	mIRC 6.0-6.0 2	A buffer overflow vulnerability exists in the '$asctime' identifier due to the way overly long format specifier strings are handled, which could let a malicious user execute arbitrary script code.	Upgrade available at: http://www.mirc.com/get.html	mIRC ASCTime Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Mantis[36]	Unix	Mantis 0.17.0-0.17.4, 0.17.4a	A vulnerability exists in several of the scripts that are used to view bug data because user permissions are not checked, which could let a malicious user obtain sensitive information.	Update available at: http://sourceforge.net/project/showfiles.php?group_id=14963	Mantis Unauthorized Bug Viewing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Mantis[37]	Unix	Mantis 0.17.0-0.17.4, 0.17.4a	A vulnerability exists in the 'View Bugs' page that list bugs from both public and private projects because user permissions are not validated, which could let a malicious user obtain unauthorized access to restricted projects.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=14963	Mantis Unauthorized Project Bug List Viewing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft [38]	Windows 95/98/ME/ NT 4.0/2000, XP	Word 2000, 2000 SR1a, 2000 SR1&2, Word 2002, Word 95, Word 97, 97 SR1&2, Word 98	A vulnerability exists when the INCLUDETEXT Field Code references a file on the local system and is included in a document, which could let a malicious user insert an arbitrary local file into a document.	No workaround or patch available at time of publishing.	Word INCLUDE TEXT Document	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft [39]	Windows NT 4.0/2000	SQL Server 2000, 2000 SP1&2	A vulnerability exists in two stored procedures within the SQL Server that allow the administrator to modify some SQL Server startup parameters and are also accessible by unprivileged users, which could let a malicious user use them in conjunction with other SQL Server vulnerabilities.	No workaround or patch available at time of publishing.	SQL Server Stored Procedure Low Privilege	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[35] uuuppz.com Advisory 002, August 27, 2002.
[36] Mantis Advisory, 2002-06, August 23, 2002.
[37] Mantis Advisory, 2002-07, August 23, 2002.
[38] Bugtraq, August 26, 2002.
[39] NGSSoftware Insight Security Research Advisory, NISR03092002A, September 3, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Microsoft [40]	Windows 95/98/MT/ NT 4.0/2000, XP	Windows 2000 Advanced Server, Advanced Server SP1-SP3, 2000 Datacenter Server, Datacenter Server SP1-SP3, 2000 Profes-sional, Profes-sional SP1-SP3, Server, Server SP1-SP3, 2000 Terminal Services, Terminal Services SP1-SP3, Windows 95, 98, 98SE, 98ME, NT Enterprise Server 4.0, Enterprise Server 4.0 SP1-SP6a, NT Server 4.0, Server 4.0 SP1-SP6a, NT Terminal Server 4.0, Terminal Server 4.0 SP1-SP6a, NT Worksta-tion 4.0, Worksta-tion 4.0 SP1-SP6a, XP 64-bit Edition, XP Home, XP Profes-sional	A vulnerability exists in the Certificate Enrollment Control, which could let a malicious delete all stored certificates on the system, including trusted root certificates, Encrypted File System (EFS) certificates, and e-mail signing certificates.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-048.asp	Microsoft ActiveX Certificate Enrollment Control Certificate Destruction CVE Name: CAN-2002-0699	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[40] Microsoft Security Bulletin, MS02-048, August 28, 2002

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Microsoft [41]	Windows 98/ME/NT 4.0/2000, XP, Mac OS 8.1 to 9.x, MacOS X	Windows 98, ME, NT 4.0, NT 4.0 Terminal Server Edition, 2000, XP, Office for Mac, Internet Explorer for Mac, Outlook Express for Mac	A vulnerability exists because due to the way the Basic Constraints field validates a digital certificate, which could let a malicious user act as a Certificate Authority and create subordinate certificates with any desired information, set up a web site that poses as a different web site, and "proving" its identity by establishing an SSL session as the legitimate web site, send e-mails signed using a digital certificate that purportedly belongs to a different user, spoof certificate-based authentication systems to gain entry as a highly privileged user, or digitally sign malware using an Authenticode certificate that claims to have been issued to a company users might trust.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-050.asp	Microsoft Certificate Validation CVE Name: CAN-2002-0862	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Microsoft [42]	Windows	Visual FoxPro 6.0	Two vulnerabilities exist: a vulnerability exists because application file extensions (.app) are not registered with Internet Explorer, which could let a remote malicious user execute database and system commands; and a vulnerability exists because specially constructed applications filenames can cause the application to be executed immediately without user interaction.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-049.asp	Microsoft Visual FoxPro 6.0 Automatic Application Execution CVE Name: CAN-2002-0696	**High**	Bug discussed in newsgroups and websites.
Microsoft [43]	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	A vulnerability exists when MSIE performs the same-origin check, which could let a malicious user bypass the verification process.	No workaround or patch available at time of publishing.	Internet Explorer HTML Same Origin Policy Violation	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[41] Microsoft Security Bulletin, MS02-050 V2.2, September 5, 2002.
[42] Microsoft Security Bulletin, MS02-049, September 4, 2002.
[43] Bugtraq, September 3, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Network Associates [44]	Windows 95/98/ME/ NT 4.0/2000, Unix	PGP 5.0, 5.1i, 5.5.3i for Windows, 5.5.5, 6.0.2, 6.0.2i, 6.5.1i, 6.5.3i for Windows, 6.5.3, 6.5.8, 7.0, 7.0.3, 7.0.4, 7.1.1, PGP Corporate Desktop 7.1, 7.1.1, Freeware 7.0.3	A buffer overflow vulnerability exists if a file with a long filename is encrypted or decrypted because the length of the filename is not properly checked, which could let a remote malicious user execute arbitrary code.	Patch available at: http://download.nai.com/products/licensed/pgp/desktop_security/windows/version_7.1.1/pgphotfix_outlookplugin711/PGPhotfix_OutlookLFN_20020828.zip	PGP Desktop Filename Buffer Overflow CVE Name: CAN-2002-0850	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
NullLogic [45]	Multiple	Null HTTPd 0.5	A Cross-Site Scripting vulnerability exists via a 404 error page, which could let a remote malicious user execute arbitrary script.	No workaround or patch available at time of publishing.	Null HTTPd Error Page Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Omnicron Technol-ogies Corpora-tion [46]	Windows 95/98/NT 4.0/2000, XP	Omni HTTPD 1.1, 2.0 Alpha 1&2, 2.0 9, 2.0.4-2.0.8, 2.4 Pro	Multiple Cross-Site Scripting vulnerabilities exist in some of the sample scripts, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	OmniHTTPD Sample Scripts Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Omnicron Technol-ogies Corpora-tion [47]	Windows 95/98/NT 4.0/2000, XP	Omni HTTPD 1.1, 2.0 Alpha 1&2, 2.0 9, 2.0.4-2.0.8, 2.4 Pro	A vulnerability exists in the '/cgi-bin/redir.exe' sample CGI script, which could let a malicious user execute arbitrary HTML code.	**Temporary workaround:** Remove the sample script 'redir.exe' from production systems.	OmniHTTPD Sample Application HTML Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PHP Develop-ment Team [48]	Unix, MacOS X 10.x	PHP 4.0, 4.0.1 pl2, 4.0.1 pl1, 4.0.1, 4.0.2, 4.0.3 pl1, 4.0.3-4.0.7, 4.1.0, 4.1.1, 4.1.2, 4.2.0-4.2.2	Two vulnerabilities exist in the mail() function: a vulnerability exists because user input is not properly sanitized, which could let a malicious user alter message content including mail headers; and a vulnerability exists if PHP is configured with the safe_mode option enabled, which could let a malicious user execute arbitrary shell commands or external binaries.	No workaround or patch available at time of publishing.	PHP Mail Function ASCII Control Character Header Spoofing CVE Name: CAN-2002-0986	Medium/ **High** **(High if arbitrary code is executed)**	Bug discussed in newsgroups and websites. Exploit script has been published for the safe_mode option vulnerability.

[44] Foundstone Labs Advisory, 090502-PCRO, September 5, 2002.
[45] Bugtraq, September 2, 2002.
[46] Securiteam, August 28, 2002.
[47] Bugtraq, August 25, 2002.
[48] Bugtraq, August 23, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Polycom[49]	Multiple	View Station 128 6.5.1, 7.2, 512 6 5.1, 7.2, DCP 6.5.1, 7.2, FX/VS 4000 4.1.5, H.323 6.5.1, 7.2, MP 6.5.1, 7.2, SP/SP384 6.5.1, 7.2, V.35 6.5.1, 7.2	Several vulnerabilities exist: a vulnerability exists because a null value is configured for the default password, which could let a malicious user obtain unauthorized access; a Directory Traversal vulnerability exists, which could let a malicious user obtain unauthorized access and sensitive information; a vulnerability exits because the number of login attempts made via the Telnet service are not restricted, which could let a remote malicious retrieve the administrator password and take over the system; a Denial of Service vulnerability exists when a malicious user makes multiple connections to the Telnet service; and a Denial of Service vulnerability exists when a malicious user sends overly long or malformed ICMP packets.	Contact the vendor about obtaining fixes.	ViewStation Multiple Vulnerabilities CVE Names: CAN-2002-0626, CAN-2002-0627, CAN-2002-0628, CAN-2002-0629, CAN-2002-0630	Low/ Medium/ **High** (Medium if sensitive informa-tion is obtained or unauthor-ized access is obtained) **(High if the adminis-trator password is obtained)**	Bug discussed in newsgroups and websites. There is no exploit code required for the null password vulnerability, the Telnet login attempt vulnerability, and the Denial of Service vulnerability. The Directory Traversal vulnerability can be exploited via a web browser.
Python Software Founda-tion[50]	Unix	Python 1.5.2, 1.6, 1.6.1, 2.0, 2.0.1, 2.1-2.1.3, 2.2, 2.2.1	A vulnerability exists in the 'os._execvpe' function because temporary files are created in an insecure manner, which could let a malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/p/python1.5	Python 'os._execvpe' Predictable Temporary Filename	**High**	Bug discussed in newsgroups and websites.

[49] Internet Security Systems, September 4, 2002.
[50] Debian Security Advisory, DSA 159-1, August 28, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Raxnet[51]	Multiple	Cacti 0.5, 0.6-0.6.8	Several vulnerabilities exist: a vulnerability exists because user input is not checked when performing the rrdtool 'graph' command, which could let a malicious user execute arbitrary commands; a vulnerability exists because the 'config.php' file is world-readable, which could let a malicious user take over the database; and a vulnerability exists because path checking is not performed when users enter operating system commands in the Data Input field, which could let a malicious user obtain unauthorized access. *Note: The malicious user must have administrative access to exploit some of these vulnerabilities.*	No workaround or patch available at time of publishing.	Cacti Multiple Vulnerabilities	Medium **High** **(High if arbitrary code is executed)**	Bug discussed in newsgroups and websites. The 'graphp' command vulnerability can be exploited via a web browser. There is not exploit required for the 'config.php' file and path checking vulnerabilities.
RedHat[52]	Unix	RedHat PXE Server 0.1; HP Secure OS software for Linux 1.0	A remote Denial of Service vulnerability exists when a malicious user sends arbitrary Dynamic Host Configuration Protocol (DHCP) packets to the Preboot eXecution Environment (PXE) server from a Voice Over IP (VOIP) phone.	**RedHat:** ftp://updates.redhat.com/ **Hewlett Packard:** The packages listed in RHSA-2002:162 under Red Hat Linux 7.1 i386 are installed to patch HP Secure OS Software for Linux Release 1.0.	Red Hat PXE Server Denial of Service CVE Name: CAN-2002-0835	Low	Bug discussed in newsgroups and websites.
Rob Flynn[53, 54, 55] ***More vendor updates[56]***	**Unix**	**Gaim 0.56, 0.57**	**A buffer overflow vulnerability exists in the Jabber messaging plug-in module, which could let a remote malicious user execute arbitrary code.**	**Rob Flynn:** **http://prdownloads.sourceforge.net/gaim/gaim-0.59.tar.gz** **RedHat:** **ftp://updates.redhat.com/7.1/en/os/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php**	**Gaim Jabber Plug-In Buffer Overflow** **CVE Name: CAN-2002-0384**	**High**	**Bug discussed in newsgroups and websites.**

[51] Bugtraq, September 3, 2002.
[52] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:162-12, August 30, 2002.
[53] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:107-11, August 5, 2002.
[54] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:098-14, August 5, 2002.
[55] Hewlett-Packard Company Security Advisory, HPSBTL0208-057, August 6, 2002.
[56] Mandrake Linux Security Update Advisory, MDKSA-2002:054, August 1, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Rob Flynn[57, 58, 59]	Unix	Gaim 0.56-0.59	A vulnerability exists in the URL handler in the manual browser option due to insufficient user input validation, which could let a malicious user execute arbitrary code.	**Rob Flynn:** http://prdownloads.sourceforge.net/gaim/gaim-0.59.1.tar.gz **Debian:** http://security.debian.org/pool/updates/main/g/gaim/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php	Gaim Manual Browser Command CVE Name: CAN-2002-0989	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Samba[60]	Multiple	Samba 2.2.4	A buffer overflow vulnerability exists due to improper termination of memory structures, which may let a malicious user execute arbitrary code.	Upgrade available at: http://us1.samba.org/samba/ftp/samba-2.2.5.tar.gz	Samba Improperly Terminated Struct Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[61]	Unix	7.0, 7.0_x86, 8.0, 8.0_x86	A vulnerability exists in ToolTalk because the _Tt_c_procid::set_default_ session function may cause a core dump, which could let a malicious user obtain sensitive information.	Patches available at: http://sunsolve.sun.com Patch 110287-09, Patch 110286-09	CDE ToolTalk Set Default Session Core Dump	Medium	Bug discussed in newsgroups and websites.
SWS[62]	Multiple	Simple Web Server 0.0.4, 0.0.3, 0.1.1, 0.1.0	Several vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user makes repeated requests for non-existent resources; a Denial of Service vulnerability exists when a recv() call fails; and a Directory Traversal vulnerability exists that could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SWS Simple Web Server Non-existent File Request Denial Of Service	Low/ Medium (Medium if sensitive informa-tion is obtained)	Bug discussed in newsgroups and websites. The repeated requests and Directory Traversal vulnerabilities can be exploited via a web browser.
Trevor Lee[63]	Multiple	SWServer 2.2	A Directory Traversal vulnerability exists a when a specially-crafted URL request containing hexadecimal URL encoded sequences is sent to the server, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.geocities.com/tlhome2000/download/swserver.html	SWServer Directory Traversal	Medium	Bug discussed in newsgroups and websites.
Ultimate PHP Board[64]	Multiple	Ultimate PHP Board 1.0 b, 1.0	A vulnerability exists because registration of the 'admin' account is not prevented, which could let a malicious user impersonate the administrative user.	No workaround or patch available at time of publishing.	Ultimate PHP Board Second 'admin' Account	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[57] Mandrake Linux Security Update Advisory, MDKSA-2002:054, August 1, 2002.
[58] Gentoo Linux Security Announcement, August 27, 2002.
[59] Debian Security Advisory, DSA 158-1, August 27, 2002.
[60] FreeBSD Security Notice, FreeBSD-SN-02:05, August 28, 2002.
[61] Sun Microsystems Alert, 110286-09, August 29, 2002.
[62] Bugtraq, September 3, 2002.
[63] PivX Security Advisory, August 28, 2002.
[64] Bugtraq, August 25, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
UTStar-com[65]	Multiple	BAS-1000 3.1 .10	A vulnerability exists because the firmware contains four accounts with default passwords, which could let a malicious user obtain full system privileges.	No workaround or patch available at time of publishing.	BAS-1000 Default User Account Passwords	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Webmin[66]	Unix	Webmin 0.21, 0.22, 0.31, 0.41, 0.42, 0.51, 0.76-0.80, 0.85, 0.88, 0.91-0.990	A vulnerability exists because the CGI that handles the 'remote_foreign_require' and 'remote_foreign_call' requests from other Webmin servers contain inadequate permission checks, which could let a remote malicious user execute arbitrary commands as root.	No workaround or patch available at time of publishing.	Webmin CGI Improper Permissions	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
ZMailer[67]	Unix	ZMailer 2.99.45-2.99.51	A buffer overflow vulnerability exists due to insufficient bounds checking on the hostname resolved from the IPv6 address, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/All/	ZMailer IPv6 Resolved Hostname Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

[65] Bugtraq, August 23, 2002.
[66] Securiteam, August 27, 2002.
[67] FreeBSD Security Notice, FreeBSD-SN-02:05, August 28, 2002.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between August 26 and September 5, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are ut ilizing**. During this period, 36 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

September 5, 2002	Afd-expl.c	Script which exploits the AFD Working Directory Buffer Overflow vulnerability.
September 5, 2002	Ffp.pdf	A document that describes a new technique for attacking cryptographic key authentication protocols that rely on human verification of key fingerprints. It covers the theoretical background and the generation of fuzzy fingerprints and also details on the implementation ffp [FFP] and its usage.
September 5, 2002	Netric-adv008.txt	Exploit for the AFD Working Directory Buffer Overflow vulnerability.
September 5, 2002	Phantasmagoria.tgz	Phantasmagoria hides tasks without modifying syscalls in Linux kernel v2.4 and includes a paper "Smashing The Kernel For Fun And Profit" and Proof of Concept code.
September 5, 2002	Pirch98.zip	Exploit for the Pirch98 IRC client vulnerability.
September 5, 2002	SPIKE2.6.tar.gz	An easy to use generic protocol API that helps reverse engineer new and unknown network protocols and also features several working examples. Includes a web server NTLM Authentication brute forcer and example code that parses web applications and DCE-RPC (MSRPC).
September 5, 2002	Sqltools.rar	A collection of tools for auditing MSSQL servers including SQLScanner, SQLPing, SQLCracker, SQLDOSStorm, and SQLOverflowDoS.
September 5, 2002	**Upb.admin.txt**	**Exploit information for the Ultimate PHP Board Second 'admin' Account vulnerability.**
September 4, 2002	Arirang-1.6.tar.gz	A powerful webserver security scanner with many features that checks over 700 vulnerabilities including the apache chunking bug, IIS .ida buffer overflow, and more.
September 4, 2002	Fakeap-0.3.tar.gz	Fake AP 0.3 generates counterfeit 802.11b beacon frames with random ESSID, BSSID (MAC), and channel assignments.
September 4, 2002	Netric-afd-exploit.c	Script which exploits the Multiple AFD Working Directory Buffer Overflows vulnerabilities.
September 4, 2002	Slog.c	A Linux keystroke logger without function hooking
September 4, 2002	Sqlscan.zip	SQLScan v1.0 is intended to run against Microsoft SQL Server and attempts to connect directly to port 1433 and features the ability to scan one host or an IP list from an input file, the ability to scan for one SQL account password or multiple passwords from a dictionary file, and the ability to create an administrative NT backdoor account on vulnerable hosts.
September 4, 2002	Wellenreiter-v15.tar.gz	A GTK/Perl program that makes the discovery and auditing of 802.11b wireless networks much easier and has an embedded statistics engine for the common parameters provided by wireless drivers, enabling you to view details about the consistency and signal strength of the network. Its scanner window can be used to discover access-points, networks, and ad-hoc cards.

September 2, 2002	Aspcode.c	Script which exploits the IIS v4.0, 5.0 5.1 asp.dll buffer overflow vulnerability.
September 2, 2002	Elinuxconf2.c	Proof of Concept exploit for the Linuxconf Local Buffer Overflow vulnerability.
September 2, 2002	Linuxconf.c	Proof of Concept exploit for the Linuxconf Local Buffer Overflow vulnerability.
September 2, 2002	Scrollkeeper.txt	Proof of Concept exploit for the ScrollKeeper Tempfile Symbolic Link vulnerability.
September 2, 2002	Sws_web_killer.c	Proof of Concept exploit for SWS Web Server vulnerability.
August 31, 2002	**Factosystem.txt**	**Example URL's for the Weblog Multiple SQL Injection vulnerability.**
August 31, 2002	Smb.c	Denial of service exploit for the Network Share Provider SMB Request Buffer Denial of Service vulnerability.
August 30, 2002	Iss.smb-dos.txt	Exploit for the Network Share Provider SMB Request Buffer Denial of Service vulnerability.
August 29, 2002	Calderax.txt	Proof of concept local exploit for the Caldera X 'xkbcomp' Vulnerability.
August 29, 2002	DSR-apache2.0x.c	Proof of Concept exploit for the current directory traversal design vulnerability in Apache 2.0.x - 2.0.39.
August 29, 2002	Fakedate-v1.0.tar.gz	FakeDate consists of tools and libraries for supplying a fake date, time, and alarm signals to target programs using LD_PRELOAD.
August 29, 2002	Nmap-3.10ALPHA1.tgz	A utility for port scanning large networks, although it works fine for single hosts.
August 29, 2002	Sonar-1.0BETA4.tar.gz	A network reconnaissance utility which runs all its scans from plugins and currently supported plugins are an ICMP scan and an ACK scan which can see if hosts that don't respond to ICMP are online.
August 28, 2002	Debug_Enviroment_Variables.txt	The CGI Debugger v1.0 (/cgi-bin/debug.pl) displays information that may be useful to a malicious user that includes the document root and server version information when passed a bogus argument.
August 28, 2002	**Idefense.webmin.txt**	**Exploit for the Webmin CGI Improper Permissions vulnerability.**
August 27, 2002	Adv-002-mirc.htm	Proof of Concept code for the mIRC ASCTime Buffer Overflow vulnerability.
August 27, 2002	Arp-sk-0.0.13.tgz	An ARP packet generator for Unix designed that illustrates ARP protocol flaws and applications such as ARP cache poisoning and MAC spoofing.
August 27, 2002	Asctime-poc	Proof of Concept exploit for the mIRC ASCTime Buffer Overflow vulnerability.
August 27, 2002	**Webmin-rpc-exploit.pl**	**Perl script which exploits the Webmin CGI Improper Permissions vulnerability.**
August 26, 2002	**Gdam123-expl.c**	**Proof of Concept exploit for the GDAM123 Filename Buffer Overflow vulnerability.**
August 26, 2002	Smbdie.zip	A Proof of Concept tool that crashes Windows machines with Netbios enabled by sending a specially crafted SMB request.
August 26, 2002	Unfburninhell1.0.tar.gz	A burneye cryptographic layer 1 & 2 cracker that can work together with john the ripper for password generation.

Trends

- **The Microsoft Product Support Services (PSS) Security Team has issued an alert regarding an increased level of hacking activity. These hacking attempts show similar symptoms and behaviors involving the detection of Trojans such as Backdoor.IRC.Flood and its variants, and the modification of the security policy on domain controllers.**
- **Web CGI exploits and Microsoft vulnerabilities continue to be two of the more frequent ways which external malicious sources conduct their probes in their attempt to gain access to networks.**
- **According to data compiled by its regional Global Command Centers (GCCs), which monitor and protect client networks from cyber-attacks, there has been a surge in cyber-attacks originating from Malaysia over the last quarter. The majority of these attacks were mainly Apache exploit attempts to execute arbitrary codes, which could lead to possible Denial-of-Service (DoS) attacks.**
- **The Common Desktop Environment (CDE) ToolTalk RPC database server contains a buffer overflow vulnerability that could allow a remote malicious user to execute arbitrary code or cause a denial of service. For more information see CERT® Advisory CA-2002-26, located at: http://www.cert.org/advisories/CA-2002-26.html.**
- **There has been an increase in Distributed Denial of Service (DDoS) attacks reported in the first seven months of 2002 over the number of DDoS attacks last year.**
- **The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of multiple buffer overflows in OpenSSL (Open Secure Sockets Layer). For more information, see NIPC Advisory 02-006, located at: http://www.nipc.gov/warnings/advisories/2002/02-006.htm.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

	Common Name			
1	W32/Klez	Worm	Stable	January 2002
2	W32/Yaha	Worm	Slight Increase	February 2002
3	W32/Magistr	File, Worm	Slight Increase	March 2001
4	W32/SirCam	Worm	Slight Decrease	July 2001
5	Elkern	File Infector	Slight Decrease	October 2001
6	W32/Nimda	File, Worm	Slight Increase	September 2001
7	JS Noclose.E	Trojan	Slight Increase	May 2002
8	Funlove	File	Stable	November 1999
9	W32/Hybris	File, Worm	Increase	November 2000
10	W32.Badtrans.B	Worm	Slight Decrease	April 2001

Note: Virus reporting may be weeks behind the first discovery of infection. A total 203 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 372 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

BAT_HOTCAK.A (Batch File Worm): This destructive mass-mailing batch file worm spreads via e-mail to all the recipients listed in the Microsoft Outlook address book and through IRC. It arrives in an e-mail with the following details:

- ? Subject: "Patch your system now!!"
- ? Body: by me..patch against virus and hackers. download this now.
- ? Attachment: hotcakes.bat

It also deletes the AUTOEXEC.BAT file.

HTML/Gaggle (Internet Worm): This is a worm that spreads in an e-mail message with the following attached file: "AngelDelMar.HTML." It is a dangerous worm because it deletes the files that grant access to the Windows Registry, as well as the Windows Help files. It also infects every file with an HTM extension found on the affected computer. Depending on the system date, HTML/Gaggle can display a text on the screen or change the Internet Explorer home page.

Logen.1028 (DOS Virus): This is a dangerous non-memory resident parasitic virus. It searches for EXE files in the current directory, then writes itself to the end of any EXE files. On Sunday the virus display messages and erases sectors on the hard drive.

Logen.1150 (DOS Virus): This is a dangerous non-memory resident parasitic virus. It searches for EXE files in the current directory, then writes itself to the end of any EXE files. On Sunday the virus display messages and erases sectors on the hard drive.

VBS_DAIRA.A (Aliases: VBS/Daira@MM, VBS.Daira@mm, I-Worm.Matra, VBS/SSIWG2.A.Worm, VBS.SSIWG2 worm) (Visual Basic Script Worm): This mass-mailing worm propagates via Microsoft Outlook and can infect Microsoft Word 2000 documents.

VBS_DEEV.A (Visual Basic Script Worm): This mass-mailing Visual Basic Script malware is dropped by TROJ_DEEV.A. It sends an e-mail with the following details:

- ? Subject: "Download MP3s fast..."
- ? Message Body: "Download this screen saver... look for the password and we will give you 10 free MP3s. Absolutely Free!!!"
- ? Attachment: %WINDOWS%\DESKTOP\FREEMP3.SCR

It also modifies the registry to enable its automatic execution every system startup. The modified registry appears as follows:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
  Default ="%Windows%\Desktop\FREEMP3.SCR"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runservices
  Default="%Windows%\Desktop\README.TXT.VBS"

A message box is displayed on the 2nd or 3rd day of the current month with this text, "yipee!"

VBS_EDNAV.B (Visual Basic Script Worm) This destructive Visual Basic Script worm deletes files found in the "My Documents" folder. It propagates through VBS file infection and by sending itself over e-mail via Microsoft Outlook. It sends out an e-mail with the following details:

- Subject: Network Problem
- Message Body: Due to the recent problems with the e-mail server, we have devised a program that will fix it up. You are requested to download the attached file and execute it at once. The whole setup will take 5 to 10 minutes. If your system crashes, just restart your computer and everything will be back to normal. Please follow instructions carefully.
  System Administrator
  Network Management.
- Attachment: <infected VBS file>

The worm also propagates via kazoo, a peer-to-peer application that allows users to share files over a network.

VBS_EDNAV.C (Visual Basic Script Worm): This destructive Visual Basic Script worm deletes files found in the "My Documents" folder. It propagates through VBS file infection and by sending itself over e-mail via Microsoft Outlook. It also propagates via KaZaA, a peer-to-peer file sharing utility.

VBS_EDNAV.D (Alias: VBS/Dedo@MM) (Visual Basic Script Worm): This Visual Basic Script worm spreads copies of itself through the KaZaA peer-to-peer file-sharing network. This worm also overwrites all the VBS files it finds in the infected machine with its malicious code.

VBS.Emailtips@mm (Visual Basic Script Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all contacts in the Outlook Address Book. It may arrive via e-mail with a subject line of "E-mail tips" and an htm attachment with the same name.

VBS.Melhack@mm (Visual Basic Script Worm): This is a Visual Basic script worm that spreads by e-mailing itself to all the contacts in the Windows Address Book. It also creates registry values and keys that (among other things) cause the worm to run when you start Windows. The worm visits a Web site and then downloads and runs the W32.Kamil Trojan. It modifies the mIRC script file to send itself over IRC and creates several folders and files on the host computer. VBS.Melhack overwrites files on the computer with a copy of one of its components.

VBS.Randa@mm (Aliases: I-Worm.Randa, VBS/Anjulie.gen@MM) (Visual Basic Script Worm): This is a worm that uses Microsoft Outlook to spread. It inserts itself into Visual Basic script files on your system and also attempts to perform a Denial of Service (DoS) attack against www.kaspersky.com. It arrives in via e-mail with the following characteristics:

- Subject: Hola, mira esto que te mando, es algo curioso
- Attachment: Miradadesdeelcoño.jpg.vbs

W32/Duksten (Win32 Virus): This is a virus that spreads via e-mail. The message that carries the virus tries to trick users into running the attached file, as this is presented as a utility for protecting IP addresses. This is a dangerous virus, as it infects Windows PE (portable executable) files. W32/Duksten is programmed in Assembler and is a semi-polymorphic, encrypted virus.

W32.Gink.Worm (Polymorphic Worm): This is a polymorphic worm that uses its own SMTP engine to send itself to e-mail addresses it finds in .doc, .asp, .php, .htm, and .xls files. The message has the various subject lines and attachments. When W32.Gink.Worm runs, it copies itself as:

- %windir%\%system%\GiGu.eXe
- %windir%\uGiG.eXe

It adds the value, "I-Worm.GiGu uGiG.eXe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs each time that you start Windows. The worm also creates the e-mail file, %windir%\%system%\GiGu.eml, with the worm as an attachment.

W32.Gismor@mm (Alias: W32.Gismor.Worm) (Win23 Worm): This is a worm that uses its own SMTP engine to send itself to e-mail addresses that it finds in your mailbox. The subject of the e-mail message is "Phenomenal," and the attached file is "MP3Player.exe."

W32.HLLW.Bare (Aliases: W32/Bare.worm, Worm.P2P.Bare) (Win32 Worm): This is a worm that spreads by using the KaZaA, Morpheus, eDonkey2000, and Bearshare file-sharing programs. It attempts to trick users into downloading and executing the malicious file by copying it as many file names. When W32.HLLW.Bare runs, it copies itself to the following folders using several file names:

- C:\Program Files\Morpheus\My Shared Folder
- C:\Program Files\Kazaa\My Shared Folder
- C:\Program Files\Bearshare\Shared
- C:\Program Files\Edonkey2000\Incoming

It creates the file names use various combinations of strings. The final file name also has a double extension of .asf, .asx, .mpe, .cpl, .mp3, .mpg, .gif, .jpg, .avi, or .zip, followed by .exe.

W32.HLLW.Nautic (Aliases: BKDR_NAUTIC.A, Worm.Win32.Nautical) (Win32 Worm): This is a worm that creates and shares a folder on the network. The worm then copies itself to this folder as a file name that is designed to trick users into executing the malicious files. The worm also listens for commands on one of the following ports:

- 335
- 2281
- 5679
- 9148

W32.HLLW.Icasur (Win32 Worm): This is a worm that copies itself to the shared folders of the KaZaA file-sharing program. Several variants have been found. All variants are written in the Microsoft Visual Basic programming language and may be compressed with UPX. The worm disguises itself as movies, games, porno-related programs, or as software files to trick KaZaA users into downloading the program and opening it.

W32.HLLW.Relmony (Alias: Worm.P2P.Relmony) (Win32 Worm): This is a worm that spreads by using the KaZaA file-sharing program. It is written in the Microsoft Visual Basic programming language. When W32.HLLW.Relmony runs, it copies itself to the C:\Program Files\KaZaA\My Shared folder and then attempts to copy itself as:

- C:\WINNT\System32\Config\Systemprofile\Start Menu\Programs\Startup\System.exe
- C:\Documents And Settings\All Users\Start Menu\Programs\Startup\System.exe
- C:\WINDOWS\Start Menu\Programs\Startup\System.exe

so that it runs each time that you start Windows. The worm displays a moving message box that has the following characteristics:

- Title: Real Easy Money
- Message: Make A lot of money each month! And get rid of me!!!!!! JUST CLICK ME

and the worm opens a new browser window to a web site that is predefined by the worm.

W32.HLLW.Walrain (Win32 Worm): This is a worm that attempts to spread across file-sharing networks such as KaZaA, iMesh, Morpheus, Gnutella, and NeoModus. It disguises itself as a porno-related program to trick users into downloading and opening it. W32.HLLW.Walrain is written using the Microsoft Visual Basic programming language and may be compressed with ASPack. When W32.HLLW.Walrain runs, it displays a pornographic image and then copies itself as:

- %windir%\Rain.exe
- A:\Porn Clip.exe

It copies itself to the root of all drives (except drive C) as Porn Clip.exe, creates the %windir%\Shared\ folder and makes many copies of itself in this folder using file names that it carries. So that other KaZaA users or iMesh users can download files from the %windir%\Shared folder, the worm adds the value, "ShareDir %windir%\Shared," to the registry key:

- HKEY_CURRENT_USER\Software\Kazaa\CloudLoad

It adds the values:

- Dir0 %windir%\Shared
- Dir1 %windir%\Shared
- Dir2 012345:%windir%\Shared

to the registry key:

- HKEY_CURRENT_USER\Software\Kazaa\LocalContent

It adds the values:

- DlDir0 012345:%windir%\Shared
- DlDir1 012345:%windir%\Shared
- DlDir99 012345:%windir%\Shared

to the registry key:

- HKEY_CURRENT_USER\Software\Kazaa\Transfer

It adds the value, "Dir1 012345:%windir%\Shared," to the registry key:

- HKEY_CURRENT_USER\Software\iMesh\Client\LocalContent

Due to bugs in the code it does not appear to successfully spread through Morpheus, Gnutella, or NeoModus.

W32.HLLW.Yoohoo.C (Aliases: W32.HLLW.Spear, Worm.P2P.Spear, Worm.P2P.Spear.b, W32/Spear.c.worm) (Win32 Worm): This is a worm that copies itself to the shared folders of the KaZaA, Bearshare, Morpheus, and eDonkey2000 file-sharing programs. It is written in the Borland Delphi programming language and may be compressed with UPX. When W32.HLLW.Yoohoo.C runs, it copies itself to the following folders using many different file names that the worm carries:

- C:\Program Files\Morpheus\My Shared Folder
- C:\Program Files\Kazaa\My Shared Folder
- C:\Program Files\Bearshare\Shared
- C:\Program Files\Edonkey2000\Incoming

W32.Housax.Irc (IRC Worm): This is an IRC worm that attempts to send itself to other IRC users. It may arrive as a file named MyHouse.JPG.EXE. The worm is written in the Borland Delphi programming language and is packed with UPX. When W32.Housax.Irc runs, it displays a fake error message. It also copies itself as C:\%windir%\MyHouse.JPG.EXE and then searches the registry to get the location of the mIRC installation folder. If it finds Mirc.exe or Mirc32.exe in this folder, it creates a Script.ini file to send itself to other IRC users.

W32.Hunch.H@mm (win32 Worm): This is a mass-mailing worm that modifies the Autoexec.bat file in an attempt to format drive C. It deletes files that have a randomly chosen extension.

W32.Hunch.I@mm (Win32 Worm): This is a mass-mailing worm that modifies the Autoexec.bat file in an attempt to format drive C. It deletes files that have a randomly chosen extension.

W32/Kilonce-A (Aliases: W32.HLLW.Kilonce, Worm.Win32.Kilonce, W32/Kilonce, W32/Kilonce.b.worm) (Win32 Worm): This is a worm which spreads via open local area network shares. The worm copies itself to the Windows folder as KILLONCE.EXE and creates the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\KillOnce = "C:\\KILLONCE.EXE"

so that it is run on system restart. W32/Kilonce-A also changes certain values in the registry so that the following entries are created:

- HKLM\Software\CLASSES\txtfile\shell\open\command = "C:\\NOTEPAD.EXE %1"
- HKLM\Software\CLASSES\exefile\shell\open\command = "C:\\KILLONCE.EXE "%1" %*"

The latter entry ensures that the worm is run before every EXE file. The worm attempts to open full access shares on drives C: to K:. It then finds open shares on remote computers on the network by enumerating network resources. Once appropriate shares are found, W32/Kilonce-A copies itself to the remote computers' Windows folder as REGEDIT.EXE (the original is saved as REGEDIT.EXE.SYS) and RUNDLL32.EXE (the original is saved as RUN32.EXE). The worm also copies itself as RICHED20.DLL to any folder containing a file with extension HTM and as SHDOCVW.DLL to any folder containing a file with extension DOC. It may also overwrite files with have the extension EML with a base64 encoded copy of itself. When the worm is running in the background, all programs with the letters 'AV' or 'KV' within the filename or with filename, LOAD.EXE, are suppressed on execution and then deleted. The worm also has a destructive payload. On the 13th of December the worm appends a line to AUTOEXEC.BAT so that all files and folders on drive C: are deleted on the next restart. Finally the worm may attempt to give guests administrator access on Windows NT based platforms.

W32.MagicCall (Win32 Virus): This is a virus that periodically (about every three minutes) attempts to connect to these URLs:

- http://www.zymf.com/
- http://www.csdn.net/soft/openfile.asp?kind=1&id=6398

At the same time, it tries to copy itself as A:\MagicCall.exe.

W32.Muzk.Irc (IRC Worm): This is an IRC worm that sends itself to other users who are on the same IRC channel as yourself. It is written in the Borland Delphi programming language and may be compressed with ASPack. When W32.Muzk.Irc runs, it copies itself as C:\%windir%\Sistem.exe and creates the following files:

- C:\Program Files\Lolita.mpeg
- C:\Progra~1\Lolita.mpeg
- C:\Program Files\Uninstall.txt
- C:\Configs.bat

The worm searches for C:\Program Files\Windows Media Player\Wmplayer.exe and opens the file if it finds it. Next, it adds the value, "Windows Baþlangýç Dosyasý C:\%Windir%\sistem.exe /ardexter," to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that it runs each time that you start Windows. The worm also searches for the installation folder of mIRC and changes the Mirc.ini file in that folder so that the worm can send itself to other mIRC users. It also attempts to change the Internet Explorer home page to a Web site that is predefined by the worm. It does this by setting the value to, "Start Page http:/ /www.muzikkrali.com," in the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main

W32/Oror-A (Aliases: W32/Oror@MM, W32.HLLW.Oror@mm) (Win32 Worm): This worm arrives in an e-mail with one of numerous possible subject line and message text combinations and the attached file has one of numerous possible filenames. When first executed, the worm displays a fake error message that reads: "Your version of WinZip Self-Extractor is not licensed, or the license information is missing or corrupted. Please contact the program vendor or the web site (www.WinZip.com) for additional information." The worm will attempt to copy itself to folders on local and shared drives using any of the following filenames:

- Kama Sutra.exe
- GiRlZ FoReVeR (Wow).exe
- Nikita v1.1 (Zip).exe
- Pamela Anderson (Porno Installation).exe
- Britney Spears Naked.exe
- Teen Sex Cam.exe
- Kurnikova Screensaver (6+).exe
- CrEdIt CaRdZ gEn.exe
- SeX.eXe
- Faith.exe.

The worm will always drop a copy of itself with the filename C:\Windows\Rundll16.exe and add the following registry entry so that Rundll16.exe is run when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\LoadCurrentProfile

It randomly chooses a single subfolder of the Program Files folder and places a copy of the worm in that subfolder. The filename of the new copy will be the name of the sub folder plus "16," "32," or "2K," e.g. Accessories2K.exe. An entry is added to registry key:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

which points to the copy of the worm. A large mIRC script will be created in the mIRC installation folder with the filename alias.ini, server.ini, notes.ini, or popup.ini. This script is a mIRC backdoor Trojan. Finally the worm will send itself in an e-mail to addresses retrieved from e-mails in the infected user's inbox. The worm also creates the following non-viral text files:

- C:\Windows\def12x.dll
- C:\Windows\rn3a.vxd
- C:\Windows\Winfile.dll
- C:\shares.txt

W32.Quin.Irc (Aliases: W32/Quin.worm, W32.HLLW.Quin) (Win32 Worm): This is a worm that spreads through IRC. When run, the worm copies itself as %windows%positron.exe. (Note the missing \ after %windows%.) Then it queries the registry for the location of mIRC. If mIRC is installed, the worm replaces the Script.ini with instructions to send the .exe file to anyone who joins the same channel as the infected computer. Additionally, the Script.ini contains an exploit that will automatically launch the .exe file in some older versions of mIRC.

W32.Stayrina (Win32 Worm): This is an intended mass-mailing worm. The virus attempts to send itself to all addresses in the Microsoft Outlook Address Book. The subject of the e-mail message is "THE MOST BEATIFULL EYES EVER!!!" There is no attachment. The virus drops a Visual Basic script, which performs the mass-mailing routine.

W32.Velost (Win32 Virus): This is a Win32 virus that infects .scr and .exe files on drives C through Z. It also attempts to connect to a particular Web site every time that an infected file is executed. When a file that is infected with W32.Velost is executed, the virus creates a mutex named "LostLove." If this mutex already exists, the virus executes the original file. Otherwise, it executes only the viral code. It then searches for files that have the .scr or .exe extension and appends itself to those that it finds. It then continues to search for more files to infect. After the virus has processed drives C through Z, it attempts to open http://www.wx-packs.com/lx/boy/boyhacker.htm.

W97M.Lami (Word 97 Macro Virus): This is a macro virus that infects active documents and the Normal.dot template file in Microsoft Word 97. To run its code, W97M.Lami hooks the Microsoft Word event handler that opens files. This virus consists of these three macro modules:

- ThisDocument
- Kamila
- frmAbnout

If the day is between December 28 and January 3, W97M.Lami attempts to delete files that have the .sys, .drv, .doc, .dll, and .dos extensions and which reside in the same folder as the virus.

WM97/Opey-BE (Word 97 Macro Virus): WM97/Opey-BE will set the File Properties information of infected documents as follows:

- Author = MIGUEL C CANETE
- Keywords = PAFFS 70-B

The virus will also change the Word user information to:

- UserName = PAF Technical Specialization Training School
- UserAddress = Fernando Air Base, Lipa City
- UserInitials = PAFTSTS

WORM_APART.A (Aliases: Worm.Win32.Apart.a, Win32/HLLW.Apart) (Win32 Worm): This worm propagates via local networks. It has backdoor capabilities and may perform the following actions on target systems:

- perform DoS (Denial of Service) attacks on remote systems
- download a file from a Web site
- execute the downloaded file
- steal cached passwords of MSN accounts, and .NET Messenger information as well

This worm drops a copy of itself and modifies the registry by adding an autostart entry to execute itself automatically on the next startup.

WORM_BLINKOM.A (Aliases: Worm.P2P.Blinkom, Win32/Blinkom.worm, Win32/Venzu.Worm, Win32.Venzu.A worm, BLINKCOM) (Win32 Worm): This worm propagates via shared network drives and has a built-in Simple Mail Transfer Protocol (SMTP) engine that allows it to mass mail copies of itself. It can also propagate via Internet Relay Chat (mIRC). This worm kills several firewall programs and lowers the Microsoft Office macro security settings of the infected system. It displays a message, drops several text files, and copies of itself in the infected system's root and Windows directory. This worm modifies the Desktop wallpaper so that it connects to a Hypertext Mark-up Language (HTML) file that displays this message: "you're infected."

WORM_DEEV.A (Alias: DEEV.A) (Internet Worm): This worm drops a mass-mailing file, VBS_DEEV.A, which propagates itself and this worm via e-mail using Microsoft Outlook. It was written using Borland Delphi, a high level programming language. Upon execution, the worm drops a copy of itself in the current user's desktop as FREEMP3.SCR. It also drops a VBS mass-mailer with the filename, README.TXT.VBS, in the same location. Afterwards, it displays a blank window with a title. If the system day of the week is Sunday, it displays a message box containing this text: "Its vandeed0 day! why work?" On any other day, it displays a different box with this text: "Error Reading File: Please download this file again. Please view readme.txt from your desktop first." When the user closes the blank message box, this worm re-executes the whole procedure again. The mass-mailing component, VBS_DEEV.A, propagates via e-mail using Microsoft Outlook. It sends e-mail with the following format to all addresses listed in the target user's Global Address Book:

- Subject: "Download MP3s fast..."
- Message Body: "Download this screen saver... look for the password and we will give you 10 free MP3s. Absolutely Free!!!"
- Attachment: FREEMP3.SCR

The attachment, FREEMP3.SCR, is the worm's dropped copy in the desktop. On the 2nd or 3rd day of the current system month, its dropped VBS component, VBS_DEEV.A, displays a message box. The worm creates the following registry entries that points to its dropped files, so that the worm's copy and its dropped mass-mailer auto executes at every system startup:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (Default) ="%Windows%\Desktop\FREEMP3.SCR"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices (Default)="%Windows%\Desktop\README.TXT.VBS"

The worm body contains these text strings: "vandeed0 Trojan."

WORM_DULOAD.B (Aliases: DULOAD, W32/Duload.worm.b, Worm.P2P.Duload.b) (Win32 Worm): This nondestructive worm propagates via KaZaA, a peer-to-peer application that allows users to share files over a network. Upon execution, it creates a copy of itself as SYSTEMCONFIG.EXE in the Windows System Directory. It also creates a folder named MEDIA in the Windows System directory and drops copies of itself using the various filenames to entice users to download this worm. To enable its automatic execution on every startup, it adds the following registry entries, which points to the dropped file, SYSTEMCONFIG.EXE:

- ? HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, Windows System Configure
- ? HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices Windows System Configure
- ? HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, Windows System Configure

It shares the created folder MEDIA in the KaZaA network by modifying the registry to overwrite current KaZaA settings. This makes the worm highly accessible to other users in the KaZaA network since the MEDIA folder contains the worm. The modified registry appears as follows:

- ? HKEY_CURRENT_USER\Software\Kazaa\LocalContent, DisableSharing="0"
- ? HKEY_CURRENT_USER\Software\Kazaa\LocalContent, Dir0="%SYSTEM%\Media\"
- ? HKEY_CURRENT_USER\Software\Kazaa\LocalContent, Dir1="%SYSTEM%\Media\"
- ? HKEY_CURRENT_USER\Software\Kazaa\LocalContent, Dir2="012345: SYSTEM%\Media\"
- ? HKEY_CURRENT_USER\Software\Kazaa\Transfer, DlDir0="012345: SYSTEM%\Media\"
- ? HKEY_CURRENT_USER\Software\Kazaa\Transfer, DlDir1="%SYSTEM%\Media\"
- ? HKEY_CURRENT_USER\Software\Kazaa\Transfer, DlDir99="%SYSTEM%\Media\"
- ? HKEY_LOCAL_MACHINE\Software\Kazaa\CloudLoad, Sharedir="%SYSTEM%\Media\"

%SYSTEM% refers to the Windows System directory, usually C:\Windows\System or C:\Windows\System32. This worm is written in Visual Basic and uses a simple encryption routine. The presence of a "TW" process in the Windows taskbar indicates that a system is infected with this worm.

WORM_ELITOR.A (Aliases: W32.HLLW.Elitor, Trojan.Win32.Elitor) (Win32 Worm): This is a Win32 worm that propagates via MSN Messenger. Upon execution, it checks whether there is an MSN Messenger installed in the system. If no MSN Messenger is found, it terminates itself and leaves the system unchanged. Otherwise, it installs itself in the system. It creates a copy of itself at this path:

- ? C:\WINDOWS\SYSTEM\britney spears naked.jpg.exe

Next, it creates a registry entry below so that a copy of the worm could execute at every Windows startup:

- ? HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run MSDOOD = c:\WINDOWS\SYSTEM\britney spears naked.jpg.exe"

Then, it stays resident in memory and waits for the user to send an instant message to one of the addressees in his MSN contact list. If a user opens a connection with one of his contacts for instant messaging, this worm automatically sends itself to that contact with a message. If the recipient of the file accepts it, the worm sends a reply.

Worm/P2P.Rain (Internet Worm): This is an Internet worm that uses the file exchange P2P network KaZaA and other file-sharing applications to spread itself. If executed, the worm opens a windows displaying a graphic of a model, celebrity, porn star, or other pornographic content. The graphical image will vary depending on what file is executed. It then copies itself in the \windows\ directory under the filename "Rain.exe", as well as, in the \windows\shared folder under a variety of different names associated with a celebrity, model, and pornographic material (30 files in all) in order to trick unknowning users into executing the files. Also within all local drives, floppy drives, and mapped network drives the file "Porn Clip.exe" will be dropped (i.e. C:\Porn Clip.exe, D:\Porn Clip.exe, etc.). So that it gets run each time a user restart their computer the following registry key gets added:

- ? HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Rain"="C:\\WINDOWS\\Rain.exe /Quiet"

The following key also gets created:

? HKEY_CURRENT_USER\Software\Kazaa\CloudLoad
"ShareDir"="C:\\WINDOWS\\Shared"

Worm/P2P.Rain does not contain a harmful payload.

XM97/Laroux-OP (Excel 97 Macro Virus): This virus is a variant of the XM97/Laroux-A Excel macro virus that creates the viral file PERSONAL.XLS in the XLSTART folder.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
AIM-Flood	N/A	CyberNotes-2002-16
Arial	N/A	CyberNotes-2002-08
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.AntiLam.20	**20**	**Current Issue**
Backdoor.Assasin	N/A	CyberNotes-2002-14
Backdoor.Cabro	N/A	CyberNotes-2002-17
Backdoor.Cabrotor	**N/A**	**Current Issue**
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.Cyn	**N/A**	**Current Issue**
Backdoor.Delf	N/A	CyberNotes-2002-16
Backdoor.Delf.B	B	CyberNotes-2002-16
Backdoor.Delf.C	C	CyberNotes-2002-17
Backdoor.Ducktoy	N/A	CyberNotes-2002-15
Backdoor.Easyserv	N/A	CyberNotes-2002-16
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.Expjan	**N/A**	**Current Issue**
Backdoor.Fearic	N/A	CyberNotes-2002-16
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.Kavar	N/A	CyberNotes-2002-16
Backdoor.Kryost	**N/A**	**Current Issue**
Backdoor.Laphex	**N/A**	**Current Issue**
Backdoor.Laphex.Client	**N/A**	**Current Issue**
Backdoor.Lastdoor	**N/A**	**Current Issue**
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Latinus.B	**B**	**Current Issue**
Backdoor.Miffice	**N/A**	**Current Issue**
Backdoor.Mirab	N/A	CyberNotes-2002-13
Backdoor.Mite	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Backdoor.MLink	N/A	CyberNotes-2002-16
Backdoor.Ndad	N/A	CyberNotes-2002-17
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	B	CyberNotes-2002-11
Backdoor.OptixPro.10	**10**	**Current Issue**
Backdoor.OptixPro.12	**12**	**Current Issue**
Backdoor.Osirdoor	N/A	CyberNotes-2002-17
Backdoor.Ptakks.B	N/A	**Current Issue**
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Robi	**N/A**	**Current Issue**
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Scanboot	N/A	CyberNotes-2002-17
Backdoor.Seamy	**N/A**	**Current Issue**
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Tela	N/A	CyberNotes-2002-17
Backdoor.Theef	N/A	CyberNotes-2002-15
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
Backdoor.WinShell	N/A	CyberNotes-2002-16
Backdoor.Y3KRat.15	N/A	CyberNotes-2002-17
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
Banan.Trojan	N/A	CyberNotes-2002-15
Bck/Litmus.201	N/A	CyberNotes-2002-14
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/Osiris	N/A	CyberNotes-2002-06
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Bneo.Trojan	**N/A**	**Current Issue**
Cardst	N/A	CyberNotes-2002-17
Dewin	N/A	CyberNotes-2002-08
Downloader-W	N/A	CyberNotes-2002-08
FakeGina.Trojan	N/A	CyberNotes-2002-16
Fortnight	N/A	CyberNotes-2002-10
IIS.Beavuh-Exploit	N/A	CyberNotes-2002-17
IRC.kierz	N/A	CyberNotes-2002-16
IRC-Smev	N/A	CyberNotes-2002-08
JS/NoClose	N/A	CyberNotes-2002-11
Liquid.Trojan	N/A	CyberNotes-2002-14
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
Netbus.160.Dropper	N/A	CyberNotes-2002-17
PWS-AOLFake	N/A	CyberNotes-2002-15
PWS-MSNCrack	**N/A**	**Current Issue**
PWS-MSNSteal	N/A	CyberNotes-2002-17
PWS-Ritter	N/A	CyberNotes-2002-16

Trojan	Version	CyberNotes Issue #
PWSteal.Kaylo	N/A	CyberNotes-2002-17
PWSteal.Netsnake	N/A	CyberNotes-2002-17
PWSteal.Profman	N/A	CyberNotes-2002-17
PWSteal.SoapSpy	**N/A**	**Current Issue**
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
RCServ	N/A	CyberNotes-2002-10
Reboot-R	**N/A**	**Current Issue**
StartPage-B	N/A	CyberNotes-2002-16
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/Zirko	N/A	CyberNotes-2002-10
Troj/Apher-A	N/A	CyberNotes-2002-17
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/Flood-O	N/A	CyberNotes-2002-14
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Ritter-A	N/A	CyberNotes-2002-17
Troj/Tobizan-A	N/A	CyberNotes-2002-16
Troj/Unreal-A	N/A	CyberNotes-2002-16
TROJ_DOAL.A	N/A	CyberNotes-2002-14
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMBNUKE.A	**N/A**	**Current Issue**
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_SUOMIA.A	**N/A**	**Current Issue**
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Adnap	N/A	CyberNotes-2002-17
Trojan.Allclicks.A	N/A	CyberNotes-2002-13
Trojan.Beway	N/A	CyberNotes-2002-15
Trojan.Crabox	N/A	CyberNotes-2002-17
Trojan.DiabKey	**N/A**	**Current Issue**
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Junnan	N/A	CyberNotes-2002-16
Trojan.Portacopo:br	N/A	CyberNotes-2002-16
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.Starfi	N/A	CyberNotes-2002-16
Trojan.Win32.Filecoder	**N/A**	**Current Issue**
Trojan.Win32.MSNTrick	N/A	CyberNotes-2002-17
VBS.Zevach	N/A	CyberNotes-2002-15
VBS_CHICK.B	N/A	CyberNotes-2002-07
W32.Alerta.Trojan	N/A	CyberNotes-2002-05

Trojan	Version	CyberNotes Issue #
W32.Azak	N/A	CyberNotes-2002-16
W32.Cbomb	N/A	CyberNotes-2002-16
W32.Click	N/A	CyberNotes-2002-15
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	N/A	CyberNotes-2002-14
W32.IRCBot	N/A	CyberNotes-2002-14
W32.Kamil	N/A	CyberNotes-2002-16
W32.Kotef	N/A	CyberNotes-2002-16
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Nuker.Winskill	N/A	CyberNotes-2002-15
W32.Tendoolf	N/A	CyberNotes-2002-09
W32.Wabbin	N/A	CyberNotes-2002-15
WbeCheck	N/A	CyberNotes-2002-09
Winshell	N/A	CyberNotes-2002-15

Backdoor.AntiLam.20 (Aliases: Backdoor.Antilam.20.b, BackDoor-AJW): This is a Backdoor Trojan that is a variant of Backdoor.AntiLam. It gives a malicious user unauthorized access to an infected computer. Backdoor.AntiLam.20 is a Delphi application, packed with UPX v1.05-1.22. The Backdoor Trojan will listen for connections on TCP ports 29999 and 47891.

Backdoor.Cabrotor: This is a backdoor Trojan program (it is a hidden remote control Trojan). The Trojan is a Windows PE EXE file written in Delphi. The original Trojan package contains three main executable files:

- CaBrONaToR.exe - client to send commands to remote server
- CaBrONeDiT.exe - server editor to modify default server settings
- 8======D.exe - server (Trojan itself)

When run, the backdoor code copies itself to the Windows directory and registers itself in the system registry in the auto-run section. In different backdoor versions the backdoor EXE name and registry keys are different. The registry key entries it makes are:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

The Trojan then opens a connection to its master's IRC channel and waits for its master's commands. The backdoor program performs following commands:

- Reports computer info (Windows version, CPU type, UserName, CompanyName etc.)
- Open/closes CD drive
- Reports directories and file names in there
- Runs a local file or executes a command
- Sends information: RAS, MS Messenger and .NET services
- Exits Windows - downloads a requested file
- Performs DoS attack to requested victim address
- Terminates itself

Backdoor.Cyn (Aliases: Backdoor/Win32.Cyn.2_1, Backdoor.Cyn.21.a, BackDoor-PB): This is a backdoor Trojan that gives a malicious user unauthorized access to an infected computer. By default, it opens ports 15432 and 51234 on the compromised computer. It is a Delphi application and is packed with UPX v1.05-1.22. When Backdoor.Cyn runs, it copies itself as %windir%\Read101.exe. The Trojan creates the value. "User32 %WinDir%\Read101.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts each time that you start Windows. The Trojan attempts to disable some antivirus and firewall programs by terminating the active processes. It intercepts confidential information by hooking keystrokes. This permits Backdoor.Cyn to steal confidential messages that you type on a compromised computer. After Backdoor.Cyn is installed, it notifies the client side using ICQ pager and establishes a connection with the malicious user through a password-protected authorization.

Backdoor.Expjan (Aliases: Explorer Trojan, BackDoor-AJZ): This is a backdoor server (Trojan) that allows unauthorized access to the infected computer. It uses the same icon as Internet Explorer. By default it opens port 2090 on the infected computer. When Backdoor.Expjan runs, it adds the value, "Explorer <path to the Trojan>," to the registry key:

- ? HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Backdoor.Kryost: This is a backdoor Trojan that allows unauthorized access to an infected computer through MSN Messenger. It allows remote execution of files and the opening and closing of the CD-ROM drive. The Trojan attempts to delete antiviral software files. When Backdoor.Kryost runs, it sends an e-mail message to the virus author to indicate that the infected computer has been compromised. Next it attempts to capture MSN Messenger commands that perform the remote execution of files may also send vulgar messages to contacts using MSN Messenger.

Backdoor.Laphex (Alias: Backdoor.Institon.11): This is a backdoor server (Trojan) that allows unauthorized access to the infected computer. Depending on the default settings inside the Trojan, it can open any port on the compromised computer. When Backdoor.Laphex runs, it does the following: it opens a predefined port for backdoor access and creates these files:

- ? %windir%\installname.exe
- ? %windir%\installname.dll.

It adds the value, "installname %windir%\installname.exe," to the registry key:

- ? HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs each time that you start Windows.

Backdoor.Laphex.Client (Aliases: BKDR_LAPHEX.A, Backdoor.Laphex, Backdoor.Trojan.Client): This is a backdoor client that allows unauthorized access to an infected computer that is running the Backdoor.Laphex server component. This client program allows its user to define the server address and port on which the client looks for a running Backdoor.Laphex server (the compromised computer). It can also upload a file to the Windows folder (the location in which the server is installed) of the compromised computer and can download URLs and files from the compromised computer. This client program can create a small server component, and its user can either use its default values or configure the following values (the program's default values are shown in brackets):

- ? The file name for the new dropped server component (Institution.exe)
- ? The port on which it listens (5152)
- ? The ICQ number for notifications
- ? The Password for the server (Aphex!).

This dropped server component name is Server.exe. When you open the Backdoor.Laphex.Client program, you see a message containing "Legal Agreement" and it asks you if you agree to these terms of use? If you click Yes, Backdoor.Laphex.Client adds the value, "institutionlegal 0x00000000 (0)," to the registry key:

- ? HKEY_LOCAL_MACHINE\SOFTWARE

This value is later used to check whether the client user has agreed the terms of the Backdoor.Laphex.Client program. If it does not find this value, it displays the message again.

Backdoor.Lastdoor (Alias: Backdoor.Lastdoor.10): This is a backdoor Trojan horse that gives the malicious user unauthorized access to the infected computer. In an effort to fool you into thinking that it is a legitimate file, this Trojan uses the same icon as the legitimate Windows file named Rundll32.exe. When Backdoor.Lastdoor runs, it copies itself as %system%\Rundll32.exe. This overwrites the original Rundll32.exe file if it is in the %system% folder. The Trojan then adds the value, "Rundll32 %system%\Rundll32.exe," to the registry key:

- ? HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

so that it runs each time that you start Windows. This Trojan opens port 16322 and waits for a connection. When a connection has been made, the malicious user can gain control of the system.

Backdoor.Latinus.B (Alias: BackDoor-KF): This is a Backdoor Trojan that gives a malicious user unauthorized access to an infected computer. By default it opens ports 55665 and 55666 on the compromised computer. The functionality of Backdoor.Latinus.B derives from Backdoor.Latinus. When Backdoor.Latinus.B runs, it copies itself as C:\Windows\System\Avpdll32.exe. The path and file name is hard-coded into the Trojan; as a result, the Trojan affects only computers that are running Windows 95/98/ME. The Trojan adds the value, "AVP monitor script C:\Windows\System\avpdll32.exe," to the registry key:

? HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs each time that you start Windows. The Trojan registers itself as a service process so that it continues to run after you log off. Backdoor.Latinus.B closes only when you shut down the system. The Trojan also notifies the client side using ICQ pager. The Trojan's functionality allows the malicious user to perform any of the following actions:

- ? Deliver system and network information to the malicious user, including login names and cached network passwords
- ? Print text, play media files, and open or close the CD-ROM drive
- ? Hide icons, the system tray, buttons, and the taskbar
- ? Switch the monitor off and on
- ? Intercept confidential information by hooking keystrokes; it also intercepts information that appears on the screen and delivers it to the malicious user.

Backdoor.Miffice (Alias: BackDoor-AJY): This is a backdoor server (Trojan) that allows unauthorized access to the infected computer. It is written in Dephi and packed with UPX. By default it opens port 1533 on the infected computer. When Backdoor.Miffice runs, it copies itself as %system%\MsOffice.exe. The Trojan adds the value, "Ms Office C:\windows\system\MsOffice.exe," to the registry key:

? HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs each time that you start Windows.

Backdoor.Mite (Aliases: TROJ_MITE.A, Backdoor-AJX): This is a backdoor Trojan with a password stealing component that is disguised as Internet banking software. If the Trojan runs, it pretends to install the Banco Brazil Internet banking software while actually installing itself. It creates these malicious files:

- ? C:\Windows\System\Setup.exe
- ? C:\Windows\System\Dosprmt.exe
- ? C:\Windows\System\Ttwain.dll

The backdoor component listens on port 61000 for incoming connections.

Backdoor.OptixPro.10: This is a backdoor Trojan that gives a malicious user unauthorized access to an infected computer. It is a Delphi application, packed with UPX v1.05-1.22. By default it opens port 3410 on the compromised computer.

Backdoor.OptixPro.12: This is a backdoor Trojan that gives a malicious user unauthorized access to an infected computer. By default it opens port 3410 on the compromised computer.

Backdoor.Ptakks.B: This is a backdoor Trojan that gives a malicious user unauthorized access to an infected computer. By default, it opens port 8012 on the compromised computer. Backdoor.Ptakks.B is a Visual C++ application, packed with UPX v0.76.1-1.22. When Backdoor.Ptakks.B runs, it displays the message, "Header file corrupt, if you downloaded this file from Internet, try to download again." It copies itself as %system%\Winxpsh.exe. Next, it creates the value, "WinXpsh VXP skinheads WinXPsh.exe," in the registry key:

? HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start or restart Windows. If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process to continue to run after you log off. In this case, Backdoor.Ptakks.B closes only when you shut down the system. The Trojan installs hook procedures into a hook chain to monitor the system for keyboard and mouse messages. The hook procedures process the

messages and pass the hook information to the next hook procedure in the current hook chain. This permits Backdoor.Ptakks.B to intercept keystrokes. The Trojan notifies the client side using ICQ pager or e-mail. The commands allow the malicious user to perform any of the following actions:

- ? Deliver system and network information to the malicious user , including login names and cached network passwords
- ? Print text, play media files, and open or close the CD-ROM drive
- ? Hide icons, the system tray, buttons, and the taskbar
- ? Switch the monitor off and on
- ? Intercept confidential information by hooking keystrokes and intercepting information that appears on the screen, and delivering it to the malicious user

Reboot-R (Alias: Trojan.WinNT.Reboot): This Trojan shuts down the host machine upon execution and at subsequent Windows startup. It utilizes a system tool that is only included with Windows XP (by default). When run on the victim machine, the Trojan uses a system tool (C:\windows\system32\shutdown.exe that is hardcoded in the Trojan) to shutdown the victim machine in 60 seconds. A fake comment is passed to the tool. The Trojan also copies itself to the Windows Startup directory as 'rundll32.exe' to run at subsequent system startup (causing a reboot loop):

- ? C:\Documents and Settings\All Users\Start Menu\Programs\Startup\rundll32.exe

On non-XP machines, the Trojan copies itself to the Windows Startup folder as above, but is rendered harmless due to shutdown.exe not being installed (by default). A system error message is observed.

Backdoor.Robi (Alias: Backdoor.Institon): This is a backdoor server that allows unauthorized access to the infected computer. By default it opens port 6969 on the compromised computer. When it runs, it creates the files %windir%\Systemrun.exe and %windir%\Systemrun.dll. Under certain circumstances, it may also create %windir%\Server.exe. It adds the value, "Systemrun %windir%\systemrun.exe," to the registry key:

- ? HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that it runs each time that you start Windows.

Backdoor.Seamy (Aliases: BackDoor-AJH, TROJ_RODASIVA.A, Backdoor:Win32/Stitch): This is a backdoor Trojan that gives a malicious user unauthorized access to an infected computer. It displays images of the Disney character Stitch and copies itself as %system%\Tws_32.exe. Next, it creates the value. "atti %system%\tws_32.exe 2," in the registry key:

- ? HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. When Backdoor.Seamy establishes a connection with the malicious user, it allows the malicious user to perform any of the following actions:

- ? Deliver system and network information to the malicious user
- ? Open or close the CD-ROM drive
- ? Hide icons, the system tray, buttons, and perform other annoying actions
- ? Download and execute

Bneo.Trojan (Alias: MSN.Trojan): Bneo.Trojan is a group of Trojan horses that are created specifically to work under MSN Messenger. Some variants of this Trojan might also open ports to allow a malicious user to gain access to the infected computer.

TROJ_SMBNUKE.A (Alias: Exploit-SMBDie: This is an attack tool that exploits the "Unchecked Buffer in Network Share Provider Can Lead to Denial of Service" vulnerability (MS02-045). When an attacker specifies an IP Address and NETBIOS name, the tool sends a malformed SMB request that causes WinNT/2K/XP systems to crash.

PWS-MSNCrack: This is a MSN Messenger password-stealing Trojan that targets the Spanish version of Windows and MSN Messenger. If the local user is logged into MSN Messenger when the Trojan is run, the user will be disconnected and the Trojan's GUI (graphical user interface) is displayed. It is designed to trick the user into thinking that they are logging back on to MSN Messenger, when in fact the username and password the enter in to the Trojan Window is sent to the author instead.

PWSteal.SoapSpy: This is password-stealing Trojan that collects user passwords, intercepts keystrokes, and submits the stolen information the author of the Trojan. PWSteal.SoapSpy is a Visual C++ application, packed with UPX v0.76.1-1.22. When PWSteal.SoapSpy runs, it copies itself as %system%\Scanreg.exe. The Trojan copies the following files to your computer:

- %system%\Sconfig.dll (not malicious)
- %system%\Date.vxd (not malicious)
- %system%\Sclg32.ocx (not malicious)
- %system%\Winload.exe (not malicious)
- %system%\Sysconf.dll (detected as PWS.Hooker.Trojan)

The Trojan alters the value, "Shell Explorer.exe scanreg.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

so that it runs each time that you start Windows. It attempts to disable some firewall programs by terminating the active processes. If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process so that it continues to run after the user logs off. In this case, PWSteal.SoapSpy will close only when the system is shut down. The Trojan retrieves the properties of the current default phonebook file. It then retrieves the following connection information for the last successfully established RAS connection:

- The phone number
- The user's user name
- The user's password

If the operating system is Windows 95/98/ME, the Trojan obtains access to the password cache that is stored on the local computer. The cached passwords include modem and dial-up passwords, URL passwords, share passwords, and others. The Trojan uses this information to authenticate its access to the remote access server. The Trojan installs hook procedures into a hook chain to monitor the system for keyboard and mouse messages. These hook procedures process the messages and pass the hook information to the next hook procedure in the current hook chain. This permits PWSteal.SoapSpy to intercept keystrokes.

TROJ_SUOMIA.A: Upon initial execution, this Trojan drops a file, MIAOUS3.EXE in the Temp directory in the following path:

- C:\WINDOWS\TEMP\

The Trojan executes itself by spawning the registry shell. Registry shell spawning executes a particular Trojan when a user tries to run an EXE, a PIF, a COM, a BAT, or an HTA file. In this case, the Trojan file, MIAOUS3.EXE is always executed whenever an executable or *.EXE file is run. The Trojan does this by first adding the registry settings:

- HKEY_CLASSES_ROOT\exefile AlwaysShowExt ""
- HKEY_LOCAL_MACHINE\Software\CLASSES\exefile AlwaysShowExt ""

Afterwards, the Trojan modifies the following registry entries:

- HKEY_CLASSES_ROOT\exefile @ "Application"
- HKEY_CLASSES_ROOT\exefile\shell\open\command @ ""%1" %*"
- HKEY_CLASSES_ROOT\exefile\DefaultIcon @ "%1"
- HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command @ ""%1" %*"
- HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\DefaultIcon

When the file, MIAOUS3.EXE is executed, a pornographic picture is displayed. However, when the path and filename, "C:_cd_N5\secret\MIAOUS3\MIAOUS3.exe," cannot be found, a system error will be displayed.

Trojan.DiabKey (Aliases: Trojan.Spy.DiabloKeys.22.A, Keylog-Diablo): This is a Trojan horse that logs keystrokes, steals passwords, and delete files. It is written in Microsoft Visual Basic version 6. When Trojan.DiabKey runs, it copies itself as %windir%\Win32dll.exe. The following files are created:

- %system%\Nmail.dll
- %system%\CheatID.exe
- %system%\CheatNeopets105.dll
- %system%\Kbget.sys

It deletes Regedit.exe, Msconfig.exe, and Regedt32.exe and creates the value, "Win32dkk %windows%win32dll.exe," in the following registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

It adds following line to the Win.ini and System.ini files:

- [windows]
- run=%WINDOWS%WIN32DLL.EXE

The Trojan then attempts to log your keystrokes into the file %system%ROB_<date>_1.RJC, where <date> is the current date. It also steals RAS passwords and stores them in the file %system%VAR_<date>_1.RJC. After Trojan.DiabKey is installed, it notifies the malicious user using ICQ pager.

Trojan.Win32.Filecoder: This is a Trojan program that renames and encrypts files into subdirectories of local and network drives. It is written in Delphi and compressed by the UPX utility. This virus program is sent via e-mail, proclaiming itself to be "a very useful tool." The program copies itself under the WINDOWS\system\NTFS.exe name and sets itself into the system registry auto-run key:

- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
  "FsystemTracer"="C:\\WINDOWS\\system\\NTFS.exe"

Once this is done, the program looks for the file with the name, "EXEADDED," and executes it. The program scans all files into all subdirectories except the directory and then alters them. It renames EXE files and writes itself under the original file name. The new name of the file contains the string:

- "EXEADDED" + old file name

For the rest files, the program renames and encrypts them. It can only rename files without encryption. The new name of the file contains the string:

- "FILEISENCODED" + old file name

The Filecoder program creates 50 different files with corrupted names in the directory named Common Desktop. These files contain Russian text.